PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-138674
(43)Date of publication of application : 16.05.2000

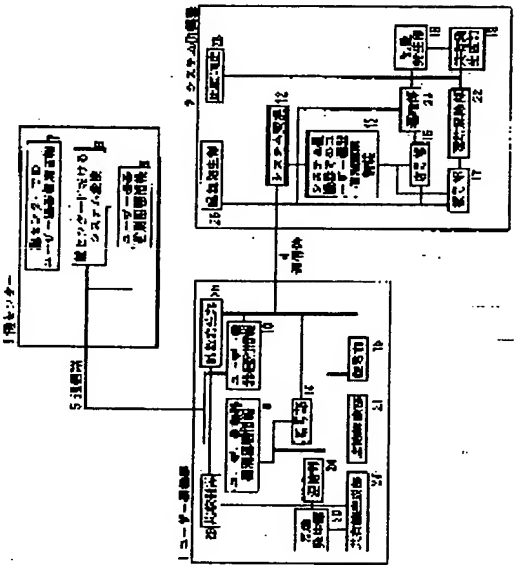
(51)Int.Cl. H04L 9/32
G07B 15/00
H04L 9/08

(21)Application number : 10-324448
(22)Date of filing : 30.10.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : KAWASAKI AKIHISA
TATEBAYASHI MAKOTO

(54) EQUIPMENT AUTHENTICATION AND CIPHER COMMUNICATION SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide the equipment authentication and the cipher communication system where a new common key is extracted and cipher communication is conducted by mutually exchanging a separate random number between a user equipment and a system side equipment in matching with an authentication phase of a challenge response using a common key crytographic algorithm.
SOLUTION: Each of n-sets of user side equipment 1 has user equipment individual information issued by a key center 3, the user equipment individual information is transferred to a system side equipment 2, the system side equipment 2 receiving this user equipment individual information extracts user equipment individual secret information from the user equipment individual information, confirms the possession of the user equipment individual secret information based on a challenge response utilizing the common key crytographic algorithm so as to authenticate the validity of the user side equipment 1 and conducts cipher communication by using the user equipment individual secret information.



LEGAL STATUS

[Date of request for examination] 19.08.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－138674
（P2000－138674A）
(43)公開日　平成12年５月16日(2000.5.16)

(51)Int.Cl.'	識別記号	FI		テーマコード'（参考）
H04L 9/32		H04L 9/00	675A	5J104
G07B 15/00	510	G07B 15/00	510	
H04L 9/08		H04L 9/00	601D	
			601E	

審査請求　未請求　請求項の数９　ＦＤ　（全８頁）

(21)出願番号　特願平10－324448

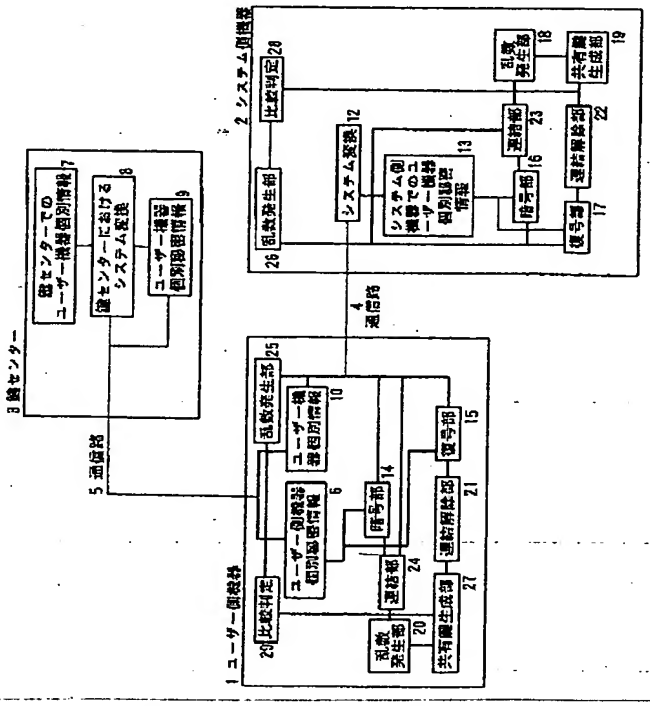
(22)出願日　平成10年10月30日(1998.10.30)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　川崎　晃久
神奈川県横浜市港北区綱島東四丁目３番１号　松下通信工業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100099254
弁理士　役　昌明　（外３名）

Ｆターム(参考)　5J104 AA01 AA07 AA16 EA01 EA16
EA24 KA02 KA04 KA06 PA01

(54)【発明の名称】　機器認証および暗号通信システム

(57)【要約】
【課題】　共通鍵暗号アルゴリズム利用のチャレンジレスポンスの認証フェースに合わせてユーザー機器とシステム側機器の間で別途の乱数を相互交換することにより新たな共有鍵を取り出し、その上で暗号通信を行なう機器認証および暗号通信システムを提供する。
【解決手段】　ｎ個のユーザー側機器１の各々は鍵センター３の発行したユーザー機器個別情報を有し、このユーザー機器個別情報をシステム側機器２に転送し、このユーザー機器個別情報を受け取ったシステム側機器２はユーザー機器個別情報からユーザー機器個別秘密情報を取り出して、共通鍵暗号アルゴリズム利用のチャレンジレスポンスによりこのユーザー機器個別秘密情報を有していることを確認することによりユーザー側機器１の正当性を認証するとともに上記共有したユーザー機器個別秘密情報を用いて暗号通信を行なう。



【特許請求の範囲】

【請求項１】　ｎ個のユーザー側機器とｍ個のシステム側機器と全機器の正当性を管理する鍵センターからなる機器認証システムであり、ｎ個のユーザー側機器の各々は前記鍵センターの発行したユーザー機器個別情報とこのユーザー機器個別情報に対応したユーザー機器個別秘密情報を有し、ユーザー機器個別情報をシステム側機器に転送し、このユーザー機器個別情報を受け取ったシステム側機器はユーザー機器個別情報から前記ユーザー機器個別秘密情報を生成して、共通鍵暗号アルゴリズム利用のチャレンジレスポンスによりこのユーザー機器個別秘密情報を有していることを確認することによりユーザー側機器の正当性を認証するとともに前記共有したユーザー機器個別秘密情報を用いて暗号通信を行なうことを特徴とする機器認証および暗号通信システム。

【請求項２】　前記システム側機器は前記鍵センターが発行したシステム側機器秘密情報を有し、前記ユーザー機器個別情報からユーザー機器個別秘密情報を生成するためには前記システム機器秘密情報が必要であるようにユーザー機器個別情報を構成し、前記ユーザー側機器は共通鍵暗号アルゴリズム利用のチャレンジレスポンスにより前記システム側機器が前記ユーザー機器個別秘密情報を有していることを確認することによりシステム側機器の正当性を認証するとともに前記共有したユーザー機器個別秘密情報を用いて暗号通信を行なうことを特徴とする請求項１に記載の機器認証および暗号通信システム。

【請求項３】　前記システム側機器は秘密鍵暗号アルゴリズムを有し、前記ユーザー機器個別情報に対して秘密鍵を用いてシステム変換を行なうことにより前記ユーザー機器個別秘密情報を生成することを特徴とする請求項１および２のいずれかに記載の機器認証および暗号通信システム。

【請求項４】　前記システム側機器および前記ユーザー機器は、独自に保有する秘密情報を相互に交換することで共有した情報を用いて暗号通信を行なうことを特徴とする請求項３に記載の機器認証および暗号通信システム。

【請求項５】　前記システム側機器および前記ユーザー機器は、独自に保有する秘密情報を相互に交換し、これらの情報を連結することにより、あらたな秘密情報を生成し、この情報をもとに暗号通信を行なうことを特徴とする請求項４に記載の機器認証および暗号通信システム。

【請求項６】　前記システム側機器および前記ユーザー機器は、相互に交換し連結された情報をユーザー機器個別秘密情報により暗号化して秘密情報を生成し、この情報をもとに暗号通信を行なうことを特徴とする請求項５に記載の機器認証および暗号通信システム。

【請求項７】　前記システム側機器および前記ユーザー機器は、それぞれ独自に乱数を生成し、この情報を別個の秘密情報として相互に交換し、交換した乱数をあらかじめ取り決めた手順により結合することにより前記システム側機器と前記ユーザー機器に固有の秘密情報を共有することで秘密通信を行なう請求項６に記載の機器認証および暗号通信システム。

【請求項８】　前記システム側機器および前記ユーザー機器は、それぞれ独自に乱数を生成し、この乱数に対しシステム側機器および前記ユーザー機器各々の固有情報をあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報として、相互に交換し、次いで、この連結された情報を前記請求項１または前記請求項２または前記請求項３に記載の手段により共有したユーザー機器個別秘密情報により復号し、あらかじめ取り決めた手順により連結を解除し、相互に交換した乱数を前記請求項７に記載の乱数と同様に個別の秘密情報として前記システム側機器と前記ユーザー機器に固有の共有することで秘密通信を行なう請求項７に記載の機器認証および暗号通信システム。

【請求項９】　前記システム側機器および前記ユーザー機器は、それぞれ独自に乱数を生成し相互にこの乱数を交換し、次いで、この乱数に対しシステム側機器および前記ユーザー機器各々で新たに独自に乱数を生成しこれをあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報として、相互に交換し、次いで、この連結された情報を前記請求項１または前記請求項２または前記請求項３に記載の手段により共有したユーザー機器個別秘密情報により復号し、あらかじめ取り決めた手順により連結を解除し、相互に交換した乱数を前記請求項７に記載の乱数と同様に個別の秘密情報として前記システム側機器と前記ユーザー機器に固有の共有することで秘密通信を行なう請求項８に記載の機器認証および暗号通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は多数のユーザー側機器とシステム側機器の間で互いに相手の正当性を確認し、当該の機器以外には秘密にデータを送受信する機器認証および暗号通信システムに関するものである。

【０００２】

【従来の技術】一般に価値のあるデータを通信相手に伝送する場合に通信相手の機器が正当なものであることを確認することが必要であり、また通信路上のデータが第三者から秘密にしなければならず、また通信路上で不正な改ざんが行なわれないようにしなければならない。そのような通信セキュリティ機能が必用となる典型的な例として無線通信を用いた高速道路の自動料金収受システムがある。

【０００３】このシステムは高速道路の料金の支払いを車に備えられる車載機と料金所ゲートに備えられる路側機との間の通信により行なうものである。ここで車載機はユーザー側機器であり路側機はシステム側機器である。車載機には着脱可能なICカードが備えられる。ICカードにはプリペイドカードの機能を持ち当初所定の金額（例えば１万円）を示す残額情報が記載されている。

【０００４】高速道路の入り口のゲート（以下入路ゲートと呼ぶ）においては車載機から車載機のID番号が路側機に通信され、路側機から車載機に入路情報（ゲートID、入路時刻など）が通信されこれがICカードに記録される。

【０００５】一方、出口のゲート（以下出路ゲートと呼ぶ）においては車載機から路側機に入路情報と残額情報が通信され、路側機では入路情報から高速道路の利用料金を計算し上記残額情報からその利用料金を差引いて残額情報を更新し、これを車載機に通信する。残額が所定の値に満たない場合は未払い処理を行なう。

【０００６】このように無線通信を用いて高速道路の利用料金の支払いを行なうことにより入出路ゲートにおける交通の混雑を軽減しようとするものである。システム中に存在する車載機の数は数100万台、路側機の数は数1000であることが想定される。

【０００７】このシステムが首尾良く運用されるために、誤まりのない高速な無線通信が実現されることは当然であるが、それ以外にも次のようなセキュリティ的な課題が解決されなければならない。

【０００８】まず、路側機は車載機が正当なものであることを認証しなければならない。偽の車載機や偽のICカードによる通信に対してはこれが偽物であることを直ちに判定しゲートを封鎖したり車両番号を記録するなどの対抗措置がとられなければならない。また、逆に車載機が路側機を正当なものであることを認証することも必要である。もし偽の路側機が車載機との通信を行なって、ICカードに記録される情報を本来あるべき区間よりも短い区間の料金に書き換えて経済的利益を得ようと試みてもそのような試みが失敗するものでなければならない。

【０００９】また、車載機と路側機の間の無線通信内容が第三者に傍受され、その内容が不正に利用されることがあってはならない。

【００１０】以上に述べた要求条件は、無線通信に認証機能および暗号機能として一般に知られる機能を付加することによって満たされる。この機能を実現する一つの手段として、車載機と路側機の間である秘密鍵暗号アルゴリズムとある秘密情報が共有されていればよい。通常この秘密情報は暗号鍵または復号鍵と呼ばれる。

【００１１】ここでシステム中に存在する車載機の台数が非常に多いことが重要である。もしもある車載機Ｘの秘密情報と車載機Ｙの秘密情報が同じものであれば、万一車載機Ｘの内容が解析され偽物の車載機Ｘ’ができたときに、この偽物Ｘ’の不正利用を排除するためにネガティブリストを用いるならば車載機Ｘ’の不正利用が防止できる。しかし同時に正当な車載機Ｙの利用まで排除されてしまう。このために車載機の秘密情報は個々の車載機毎に異なる必要がある。

【００１２】このとき、路側機は個々の車載機の秘密情報をどのように獲得するかが問題となる。一つの方法は、路側機にすべての車載機のIDと秘密情報の組みの情報を記憶することである。しかし、この方法はシステムに存在する数1000の路側機の記憶内容を更新することが大きな負担となる。また万一、一つの路側機が解析された場合すべての車載機の秘密情報がすべて暴露されるというシステムセキュリティ上の脆弱さがある。

【００１３】

【発明が解決しようとする課題】このように、従来の機器認証および暗号通信システムでシステムセキュリティを実現しようとすると、システム側機器の不正な解析によりユーザー側機器のすべてに影響を与えるという問題点を有するものであった。

【００１４】

【課題を解決するための手段】本発明は従来の機器認証および暗号通信システムにあった上記のような欠点を改善するためになされたものであり、請求項１にかかる発明は、ｎ個のユーザー側機器とｍ個のシステム側機器と全機器の正当性を管理する鍵センターからなり、ｎ個のユーザー側機器の各々は前記鍵センターの発行したユーザー機器個別情報とこのユーザー機器個別情報に対応したユーザー機器個別秘密情報を有し、そのユーザー機器個別情報をシステム側機器に転送し、このユーザー機器個別情報を受け取ったシステム側機器はユーザー機器個別情報から前記ユーザー機器個別秘密情報を取り出して、共通鍵暗号アルゴリズム利用のチャレンジレスポンスによりこのユーザー機器個別秘密情報を有していることを確認する手段を備えている。

【００１５】この構成をとることにより、システム側機器は個々のユーザー側機器の個別秘密情報をデータベースのような形で記憶することなく、ユーザー機器個別秘密情報を共有することができて、ユーザー側機器の正当性を認証するとともに、暗号通信を行なうことが可能となるという作用を有する。

【００１６】請求項２にかかる発明は、請求項１に記載の発明において、上記システム機器は上記鍵センターが発行したシステム機器秘密情報を有し、上記ユーザー機器個別情報からユーザー機器個別秘密情報を生成するにあたって上記システム機器秘密情報が必要であるようにユーザー機器個別情報を構成し、上記ユーザー側機器は共通鍵暗号アルゴリズム利用のチャレンジレスポンスにより上記システム側機器が上記ユーザー機器個別秘密情報を有していることを確認する手段を有している。

【００１７】この構成をとることにより、ユーザー機器

個別秘密情報を共有することができ、ユーザー側機器の正当性を認証するとともに、暗号通信を行なうことが可能となるという作用を有する。

【００１８】請求項３にかかる発明は、請求項１および２に記載の発明において、上記システム側機器は秘密鍵暗号アルゴリズムを有し、上記ユーザー機器個別情報に対して秘密鍵を用いてシステム変換を行なうことにより上記ユーザー機器個別秘密情報を生成する手段を有している。

【００１９】この構成をとることにより、システム側機器は個々のユーザー側機器の個別秘密情報をデータベースのような形で記憶することなく共有したユーザー機器個別秘密情報を用いてユーザー側機器の正当性を認証するとともに暗号通信を行なうことができるという作用を有する。

【００２０】請求項４にかかる発明は、請求項３に記載の発明において、上記システム側機器および上記ユーザー機器は、独自に保有する秘密情報を相互に交換することで共有した情報を用いて暗号通信を行なう手段を有している。

【００２１】この構成をとることにより、システム側機器は個々のユーザー側機器の個別秘密情報をデータベースのような形で記憶することなく、また万一システム側機器あるいはユーザー機器が解析されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがないという作用を有する。

【００２２】請求項５にかかる発明は、請求項４に記載の発明において、上記システム側機器および上記ユーザー機器は、独自に保有する秘密情報を相互に交換し、これらの情報をあらかじめとりきめた手順で連結することにより、新たな秘密情報を生成し、この情報をもとに暗号通信を行なう手段を有している。

【００２３】この構成をとることにより、万一システム側機器あるいはユーザー機器が解析されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがないという作用を有する。

【００２４】請求項６にかかる発明は、請求項５に記載の発明において、上記システム側機器および上記ユーザー機器は、相互に交換し連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報をもとに暗号通信を行なう手段を有している。

【００２５】この構成をとることにより、万一システム側機器とユーザー機器の双方向の通信が傍受されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがないという作用を有する。

【００２６】請求項７にかかる発明は、請求項６に記載の発明において、上記システム側機器および上記ユーザー機器は、それぞれ独自に乱数を生成し、この情報を別個の秘密情報として、相互に交換することで秘密通信を行なう手段を有している。

【００２７】この構成をとることにより、万一システム側機器とユーザー機器の双方向の通信が傍受されユーザー機器個別秘密情報暴露したとしても次回の暗号通信まで傍受されるおそれはないという作用を有する。

【００２８】請求項８にかかる発明は、請求項７に記載の発明において、上記システム側機器および上記ユーザー機器は、それぞれ独自に乱数を生成し、この乱数に対しシステム側機器および上記ユーザー機器各々の固有情報をあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報として、相互に交換し、次いで、この連結された情報を上記請求項１または上記請求項２または上記請求項３に記載の手段により共有したユーザー機器個別秘密情報により復号し、あらかじめ取り決めた手順により連結を解除し、相互に交換した乱数を請求項７に記載の乱数と同様に個別の秘密情報として上記システム側機器と上記ユーザー機器に固有の共有することで秘密通信を行なう手段を有している。

【００２９】この構成をとることにより、万一システム側機器とユーザー機器の双方向の通信が傍受されリプレイアタックが行なわれたとしても、その暗号通信の内容が傍受されるおそれがないという作用を有する。

【００３０】請求項９にかかる発明は、請求項８に記載の発明において、上記システム側機器および上記ユーザー機器は、それぞれ独自に乱数を生成し相互にこの乱数を交換し、次いで、この乱数に対しシステム側機器および上記ユーザー機器各々で新たに独自に乱数を生成しこれをあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報とする秘密通信を行なう手段を有している。

【００３１】この構成をとることにより、万一システム側機器とユーザー機器の双方向の通信が傍受されリプレイアタックが行なわれ、さらにユーザー機器個別秘密情報が暴露したとしても、その暗号通信の内容が傍受されるおそれがないという作用を有する。

【００３２】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。図１は、本発明の実施形態の機器認証および暗号通信システムの構成を示すブロック図である。図１において、機器認証および暗号通信システムは、基本的には、ユーザー側機器１と、システム側機器２と、全機器の正当性を管理する鍵センター３とで構成されている。具体的にはユーザー側機器１としては自動料金収受システムにおける車載機を、また、システム側機器２としては自動料金収受システムにおける路側機を念頭においている。

【００３３】鍵センター３は全体システムを管理するセンターであり、ユーザー側機器１およびシステム側機器

２又はそれらと鍵センター３と間を接続するデータ通信を行なう公開の通信路４である。公開の通信路４とは悪意のある第３者が盗聴や改ざんを行なう危険性があることを意味する。

【００３４】一方、鍵センター３とユーザー側機器１またはシステム側機器２との間を接続するデータ通信を行なう秘密の通信路５である。秘密の通信路５とは悪意のある第３者であっても盗聴や改ざんができないことを意味する。

【００３５】ユーザー側機器１はユーザー側機器個別秘密情報６を有する。本実施形態ではこのユーザー側機器個別秘密情報６を公開の通信路４を介して送信されるユーザー機器個別情報10により共有することが第１のターゲットである。

【００３６】この第１のターゲットがクリアされたならば、次に、このユーザー側機器個別秘密情報を用いて公開の通信路４を介して認証や暗号通信を行なうことが第２のターゲットである。

【００３７】一方、鍵センター３はユーザー機器個別情報７を有する。鍵センターにおけるシステム変換部８はこのユーザー機器個別情報７に対してシステム変換を行ないユーザー機器個別秘密情報９を生成する。ユーザー側機器１はこのユーザー機器個別秘密情報９およびユーザー機器個別情報７を秘密の通信路５を介して、ユーザー側機器個別秘密情報６およびユーザー機器個別情報10として保有する。

【００３８】システム側機器２は上記鍵センター３の有するシステム変換８と同等のシステム変換12を保有する。システム側機器におけるシステム変換部12はユーザー側機器１から公開の通信路４を介して通信されたユーザー機器個別情報10に対して上記システム変換８に対応する変換を行なうことにより上記ユーザー機器個別秘密情報６と同一のデータとなるユーザー機器個別秘密情報13を取り出す。取り出されたデータはシステム側機器でのユーザー機器個別秘密情報13となって格納される。以上によりユーザー機器１とシステム側機器２はユーザー機器個別秘密情報６を共有することができ、第１のターゲットがクリアされたことになる。

【００３９】ユーザー機器１は、さらに共通鍵暗号アルゴリズムの復号部15および暗号部14を有する。乱数発生部20は乱数20を発生させる。同じく乱数発生部25は乱数25を発生させる。連結部24は二つの乱数データをあらかじめ取り決められた手順で連結する機能を有する。一方、連結解除部21はこれらに対応し連結された乱数を解除する機能を有する。最後に、結合解除された乱数20とシステム側機器２から受信した乱数18を連結することでユーザー機器１とシステム側機器２との共有した秘密情報が得られる。

【００４０】システム側機器２は、この共通鍵暗号アルゴリズムの暗号部16と復号部17を有する。また、乱数発生部18は乱数18を発生させる。同じく乱数発生部26は乱数26を発生させる。また、連結部23は入力された二つの乱数データをあらかじめ取り決められた手順で連結する機能を有しており、一方、連結解除部22はこれらに対応し連結された乱数を解除する機能を有している。

【００４１】上記の実施形態における具体的な動作を、Ａ．ユーザー個別情報配送フェーズ、Ｂ．認証・鍵共有フェーズ及びＣ．暗号通信フェーズに分けて説明する。

【００４２】Ａ．ユーザー個別情報配送フェーズ

１）鍵センター３はユーザー機器個別情報７からシステム変換部８によりユーザー機器個別秘密情報を生成し、秘密の通信路５を介してユーザー機器１に送信する。

２）ユーザー機器１は、公開の通信路４を介して鍵センター３から通信されたユーザー機器個別情報10をシステム側機器２に送信する。

３）システム側機器２は、受信したユーザー機器個別情報10をシステム変換部12によりユーザー機器個別秘密情報13を生成する。

【００４３】このようにして共有したユーザー個別秘密情報を次の認証・鍵共有フェーズでは、ユーザー機器１における暗号部14と復号部15、およびシステム側機器２における暗号部16と復号部17の暗号／復号用鍵として用いる。

【００４４】Ｂ．認証・鍵共有フェーズ

４）ユーザー機器１では乱数発生部25により乱数25を発生させ、これをシステム側機器２に送信する。

５）システム側機器２では、乱数発生部18により乱数18を発生させる。

６）システム側機器２では、乱数18をユーザー機器１から送られた乱数25と連結部23において連結し、暗号部16において暗号化した後ユーザー機器１に送信する。

７）ユーザー側機器１では受信した暗号データを復号部14により復号し、連結解除部21において、乱数18と乱数25を取り出す。

８）ユーザー側機器１では、取り出した乱数18と自らの持つ乱数発生部20で生成した乱数20を共有鍵生成部19で連結し暗号通信用の秘密情報を生成する。この秘密情報を共有鍵と呼ぶ。

９）またユーザー側機器１では、取り出した乱数25と自らの持つ乱数発生部25で生成した乱数25を比較判定部29で比較判定しチャレンジレスポンスの判定を行なう。

10）システム側機器２では、乱数発生部26により乱数26を発生させ、これをユーザー機器１に送信する。

11）ユーザー機器１では、乱数発生部20により生成した乱数20をシステム側機器２から送られた乱数26と連結部24において連結し、暗号部14において暗号化した後システム側機器２に送信する。

12）システム側機器２では受信した暗号データを復号部17により復号し、連結解除部22において、乱数20と乱数26を取り出す。

13）システム側機器２では、取り出した乱数20と自らの持つ乱数発生部18で生成した乱数18を共有鍵生成部27で連結し暗号通信用の秘密情報を生成する。この秘密情報を上記８）と同様に共有鍵と呼ぶ。

14）またシステム側機器２では、取り出した乱数26と自らの持つ乱数発生部26で生成した乱数26を比較判定部28で比較判定しチャレンジレスポンスの判定を行なう。

【００４５】Ｃ．暗号通信フェーズ

15）上記したフェーズで認証が成功した場合、ユーザー側機器１およびシステム側機器２はそれぞれの持つ暗号部／復号部の鍵情報を上記した認証・鍵共有フェーズで共有した共有鍵におき換える。

16）上記共有鍵を持ったユーザー側機器１およびシステム側機器２のそれぞれの暗号部／復号部により暗号通信を行なう。

【００４６】以上に説明した実施形態においては、以下に述べる効果を有している。

１．システム側機器２は個々のユーザー側機器１の個別秘密情報をユーザー側
機器１から転送されたユーザー側機器の個別情報から生成することができるために、データベースのような形で記憶する必要がない。

２．システム側機器２でユーザー側機器１の個別秘密情報を再現するために正当なシステム側機器しか知らない秘密データを必要とするためにユーザー側機器１がシステム側機器２を認証できる。

３．乱数による鍵共有を行なうため通信量が多く比較的傍受されやすい一般通信における安全性を向上することができる。

４．チャレンジレスポンスの認証のフェースと平行して鍵共有を行なうため通信シーケンスを節約することができる。

５．逐次生成される乱数を基に認証、暗号通信を行なうため万一システム側機器あるいはユーザー機器が解析されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがない。

【００４７】

【発明の効果】以上のように、本発明の請求項１に記載の発明によれば、システム側機器は個々のユーザー側機器の個別秘密情報をユーザー側機器から転送された鍵カプセルデータから再現することができるために、個別秘密情報をデータベースのような形で記憶する必要がない。

【００４８】また、請求項２に記載の発明によれば、システム側機器でユーザー側機器の個別秘密情報を再現するために正当なシステム側機器しか知らない秘密データを必要とするためにユーザー側機器がシステム側機器を認証できる。

【００４９】また、請求項３に記載の発明によれば、システム側機器で個々のユーザー側機器の個別秘密情報をデータベースのような形で記憶することなく共有したユーザー機器個別秘密情報と秘密鍵暗号を用いてユーザー側機器の正当性を認証するとともに暗号通信を行なうことができる。

【００５０】また、請求項４に記載の発明によれば、独自に保有する秘密情報を相互に交換して共有した情報を用いることで、システム側機器は個々のユーザー側機器の個別秘密情報をデータベースのような形で記憶することなく、また万一システム側機器あるいはユーザー機器が解析されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがない。

【００５１】また、請求項５に記載の発明によれば、独自に保有する秘密情報を相互に交換し、これらの情報を連結することにより、あらたな秘密情報を生成し、暗号通信を行なうことで、万一システム側機器あるいはユーザー機器が解析されたとしてもそこで暴露された情報だけでは暗号通信を傍受されることがない。

【００５２】また、請求項に記載６の発明によれば、相互に交換し連結された情報をユーザー機器個別秘密情報により暗号化して秘密情報を生成し、この情報をもとに暗号通信を行なうことにより、万一システム側機器とユーザー機器の双方向の通信が傍受されたとしてもそこで暴露された情報だけでは暗号化を行なっている秘密情報は知り得ず、暗号通信を傍受されることがない。

【００５３】また、請求項７に記載の発明によれば、それぞれ独自に乱数を生成し、この情報を別個の秘密情報として相互に交換し、交換した乱数をあらかじめ取り決めた手順により結合することにより上記システム側機器と上記ユーザー機器に固有の秘密情報を共有することで秘密通信を行なうことにより、万一システム側機器とユーザー機器の双方向の通信が傍受されユーザー機器個別秘密情報が暴露したとしても次回の暗号通信まで傍受されるおそれはない。

【００５４】また、請求項８に記載の発明によれば、上記システム側機器および上記ユーザー機器は、それぞれ独自に乱数を生成し、この乱数に対しシステム側機器および上記ユーザー機器各々の固有情報をあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報として、相互に交換する。次いで、この連結された情報を上記請求項１または上記請求項２または上記請求項３に記載の手段により共有したユーザー機器個別秘密情報により復号し、あらかじめ取り決めた手順により連結を解除し、相互に交換した乱数を請求項７記載の乱数と同様に個別の秘密情報として上記システム側機器と上記ユーザー機器に固有の共有することで秘密通信を行なうことにより、万一システム側機器とユーザー機器の双方向の通信が傍受されリプレイアタックが行なわれたとしても、その暗号通信の内容が傍受されるおそれがない。

【００５５】また、請求項９に記載の発明によれば　上記システム側機器および上記ユーザー機器は、それぞれ独自に乱数を生成し相互にこの乱数を交換する。次いで、この乱数に対しシステム側機器および上記ユーザー機器各々で新たに独自に乱数を生成しこれをあらかじめ取り決めた手順により連結し、この連結された情報をユーザー機器個別秘密情報により暗号化した秘密情報を生成し、この情報を別個の秘密情報として、相互に交換する。次いで、請求項８と同様にこの連結された情報を上記請求項１または上記請求項２または上記請求項３に記載の手段により共有したユーザー機器個別秘密情報により復号し、あらかじめ取り決めた手順により連結を解除し、相互に交換した乱数を請求項７に記載の乱数と同様に個別の秘密情報として上記システム側機器と上記ユーザー機器に固有の共有することで秘密通信を行なうことにより、万一システム側機器とユーザー機器の双方向の通信が傍受されリプレイアタックが行なわれ、さらにユーザー機器個別秘密情報が暴露したとしても、その暗号通信の内容が傍受されるおそれがない。

【図面の簡単な説明】

【図１】本発明の実施形態における機器認証および暗号通信システムの構成を示すブロック図である。

【符号の説明】

1　ユーザー側機器
2　システム側機器
3　鍵センター
6　ユーザー側機器個別秘密情報
7　鍵センターでのユーザー機器個別情報
8　鍵センターにおけるシステム変換部
9　ユーザー機器個別秘密情報
10　ユーザー機器個別情報
12　システム変換部
13　システム側機器でのユーザー機器個別秘密情報
14、16　暗号部
15、17　復号部
18、20、25、26　乱数発生部
19、27　共有鍵生成部
21　連結解除部
22　連結解除部
23、24　連結部
28、29　比較判定部

【図1】